ELSEVIER

Discrete Mathematics 187 (1998) 291–295

DISCRETE MATHEMATICS

Note

A new upper bound for binary codes with minimum distance four

Jun Kyo Kim*, Sang Geun Hahn

Department of Mathematics, Korea Advanced Institute of Science and Technology, Gu-Sung Dong, Yu-Sung Gu, Taejon 305 701, South Korea

Received 2 June 1995; accepted 2 June 1997

Abstract

The purpose of this paper is to give an upper bound for $A[n,4]$, the maximum number of codewords in a binary code of length n with minimum distance d between codewords.

Keywords: One-error-corecting codes; Binary codes

AMS classification: 05b40; 94b65

1. Introduction

In this correspondence, we present an upper bound for $A[n,d]$, the maximum number of codewords in a binary code of length n with minimum distance d between codewords.

This function $A[n,d]$ and $A[n,d,w]$, the maximum number of codewords in a binary code of length n, minimum distance d and constant weight w, have been studied by many authors. In this section we give an upper bound for $A[n,3]$

$$A[n+1,4]=A[n,3]\leqslant\frac{2^{n+1}A[n,4,2]}{n(n+1)-6\cdot A[n,4,3]+2(n+1)\cdot A[n,4,2]}.$$

Earlier bounds on $A[n,d]$ were given in [6,8,2,1] (see also [3, Ch. 9]). They used the linear programming method, whereas we used only the elementary method.

* Corresponding author. E-mail: jkkim@crypt.kaist.ac.kr.

0012-365X/98/$19.00
PII S0012-365X(97)00199-4

2. Notations

For convenience, we define some notations and conventions used in this section. If α is a real number, then $\lfloor \alpha \rfloor$ denotes the greatest integer not exceeding α. All codes are binary codes of length n with minimum distance 3. Let n be a positive integer and $r \in \{0, 1, \ldots, n\}$. Let $C \subset \mathbb{F}^n$ be a code with codewords $A[n,3]$ where $\mathbb{F} = \{0,1\}$. We first introduce some set:

$$B_r(x) = \{y \in \mathbb{F}^n \mid d(x,y) \leqslant r\},$$

$$X = \mathbb{F}^n - \bigcup_{g \in C} B_1(g),$$

$$S = \{(x,g) \mid x \in X,\ g \in C \text{ and } d(x,g) = 2\}.$$

Let $x \in X$ and $g \in C$. We let

$$C_x = \{(x,g) \mid (x,g) \in S\} \quad \text{and} \quad X_g = \{(x,g) \mid (x,g) \in S\}.$$

Hence,

$$S = \bigcup_{x \in X} C_x = \bigcup_{g \in C} X_g. \tag{1}$$

3. Upper bounds on $A[n, 4]$

The first three theorems are well known.

Theorem 1 (Trivial cases). *Let d, w, n be integers, $d \neq 0, w \leqslant n$. Then*

(a) $A[n,d] = A[n+1, d+1]$ *if d is odd,*
(b) $A[n,d,w] = \lfloor n/w \rfloor$ *if $d = 2w$,*
(c) $A[n,d,w] = A[n, d-1, w]$ *if d is even,*
(d) $A[n,3] \cdot (n+1) \leqslant 2^n$. (2)

Theorem 2 (Johnson [6, p. 98]).

$$A[n,d,w] \leqslant \left\lfloor \frac{n}{w} A[n-1,d,w-1] \right\rfloor, \quad (n \geqslant w \geqslant 1),$$

$$A[n,d,w] \leqslant \left\lfloor \frac{n}{n-w} A[n-1,d,w] \right\rfloor, \quad (n > w \geqslant 0).$$

Theorem 3 (Kirkman [4] and Schönheim [7], see also Hall Jr. [5, p. 237]).

$$A[n,4,3] = \begin{cases} \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor & \text{if } n \not\equiv 5 \pmod 6, \\ \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor - 1 & \text{if } n \equiv 5 \pmod 6. \end{cases}$$

Now, suppose that $x \in \mathbb{F}^n$ and $g, g' \in C$. Then

$$d(x+g, x+g') = d(g, g') \geqslant 3.$$

Hence, $x + C$ is also code with minimum distance 3. We have the following lemma.

Lemma 4. *If $C \subset \mathbb{F}$ is a code with minimum distance 3, so is $x + C$.*

The next three lemmas lead us directly to the main theorem.

Lemma 5. *Let $x \in X$. Then*

$$|C_x| \leqslant A[n,4,2] = \left\lfloor \frac{n}{2} \right\rfloor.$$

Proof. From the definition of $A[n,4,2]$, Lemma 4 and Theorem 1(c), we obtain

$$\begin{aligned} |C_x| &= |\{g \in C \mid d(x,g) = 2\}| = |\{g \in C \mid d(0, g+x) = 2\}| \\ &= |\{g \in x + C \mid d(0,g) = 2\}| \leqslant A[n,3,2] = A[n,4,2]. \end{aligned}$$ □

Lemma 6. *Let $g \in C$. Then*

$$|X_g| \geqslant \frac{n(n-1)}{2} - 3 \cdot A[n,4,3].$$

Proof. From Lemma 4 and Theorem 1(c), we obtain

$$\begin{aligned} |X_g| &= |\{y \in \mathbb{F}^n \mid d(y,g) = 2\} \\ &\quad - |\{y \in \mathbb{F}^n \mid d(y,g) = 2 \text{ and } d(y,g') = 1 \text{ for some } g' \in C\}| \\ &= |\{y \in \mathbb{F}^n \mid d(y,g) = 2\}| \\ &\quad - |\{y \in \mathbb{F}^n \mid d(y,g) = 2 \text{ and } d(y,g') = 1 \text{ for some } g' \in C\}| \\ &= \frac{n(n-1)}{2} - 3 \cdot |\{g' \in C \mid d(g,g') = 3\}| \\ &= \frac{n(n-1)}{2} - 3 \cdot |\{g' \in g + C \mid d(0,g') = 3\}| \\ &\geqslant \frac{n(n-1)}{2} - 3 \cdot A[n,3,3] = \frac{n(n-1)}{2} - 3 \cdot A[n,4,3]. \end{aligned}$$ □

We proceed to show that the unions in (1) are actually disjoint unions. Hence, each $\{C_x\}$ or $\{X_g\}$ in (1) forms a partition of S. The following lemma is obvious.

Lemma 7.

(a) *For $(x_1, g_1), (x_2, g_2) \in S$, let $(x_1, g_1) \sim_1 (x_2, g_2)$ if and only if $g_1 = g_2$.*

(b) *For* $(x_1,g_1),(x_2,g_2)\in S$, *let* $(x_1,g_1)\sim_2(x_2,g_2)$ *if and only if* $x_1=x_2$.
Then $\sim_1$ *and* $\sim_2$ *are equivalence relations on* S.

Theorem 8 (Main theorem).

$$A[n+1,4]=A[n,3]\leqslant\frac{2^{n+1}A[n,4,2]}{n(n-1)-6\cdot A[n,4,3]+2(n+1)\cdot A[n,4,2]}. \tag{3}$$

Proof. Let C be a code with codewords $A[n,3]$. Using (1), Lemmas 5 and 7, we have

$$\begin{aligned}|S| &= \sum_{x\in X}|C_x|\leqslant\sum_{x\in X}A[n,4,2]\leqslant|X|\cdot A[n,4,2]\\ &= (2^n-(n+1)\cdot A[n,3])\cdot A[n,4,2].\end{aligned} \tag{4}$$

From (1) and Lemmas 6 and 7, we have

$$\begin{aligned}|S| &= \sum_{g\in C}|X_g|\geqslant\sum_{g\in C}\left[\frac{n(n-1)}{2}-3\cdot A[n,4,3]\right]\\ &= A[n,3]\left[\frac{n(n-1)}{2}-3\cdot A[n,4,3]\right].\end{aligned} \tag{5}$$

Comparison of (4) and (5) gives (3). □

The bound (3) improves the bound (2) whenever $n(n-1)>6A[n,4,3]$. This is the case if and only if $n\geqslant 3$ and $n\not\equiv 1\pmod 6$.

Proposition 9. *If* $n\geqslant 3$ *and* $n\not\equiv 1\pmod 6$, *then*

$$\frac{2^{n+1}A[n,4,2]}{n(n-1)-6\cdot A[n,4,3]+2(n+1)\cdot A[n,4,2]}+1\leqslant\frac{2^n}{n+1}.$$

Proof. From Theorem 3, we have

$$6A[m,4,3]=m(m-1)\quad\text{for } m\equiv 1\pmod 6,$$

$$6A[m,4,3]\geqslant m(m-1)+8\quad\text{for } m\geqslant 3,\ m\not\equiv 1\pmod 6.$$

Hence, from Theorem 1(b), we know

$$\begin{aligned}&\frac{2^n}{n+1}-\frac{2^{n+1}A[n,4,2]}{n(n-1)-6\cdot A[n,4,3]+2(n+1)\cdot A[n,4,2]}\\ &\geqslant\frac{2^{n+1}\cdot 8}{(8+(n+1)(n-1))(2(n+1))}\geqslant\frac{2^{n+3}}{(n+1)(n^2+7)}\geqslant 1.\end{aligned}$$ □

It is known that $A[24,4]\leqslant 344\,636$ ([1], see also [3, Ch. 9]). Theorems 1(b), 3 and the previous theorem, yield

Theorem 10.

$A[24,4] \leqslant 344\,308.$

References

[1] M.R. Best, Binary codes with a minimum distance of four, IEEE Trans. Inform. Theory IT-26 (1980) 738–742.
[2] M.R. Best, A.E. Brouwer, F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane, Bounds for binary codes of length less than 25, IEEE Trans. Inform. Theory IT-24 (1978) 81–93.
[3] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer, New York, 1988.
[4] T.P. Kirkman, On a problem in combinations, Cambridge Dublin Math. J. 2 (1847) 191–204.
[5] M. Hall Jr., Combinatorial Theory, Blaisdell: Watham, MA, 1967.
[6] S.M. Johnson, On upper bounds for unrestricted binary error-correcting codes, IEEE Trans. Inform. Theory IT-17 (1971) 203–207.
[7] J. Schönheim, On maximal system of k-tuples, Studia Sci. Math. Hungar. 1 (1966) 363–368.
[8] N.J.A. Sloane, A survey of constructive coding theory and a table of binary codes of highest known rate, Discrete Math. 3 (1972) 265–294.
[9] V.D. Tonchev, Combinatorial Configurations Designs, Codes, Graphs, Longman, New York, 1988.